

HEWLETT-PACKARD COMPANY

Intellectual Property Administration

P. O. Box 272400

Fort Collins, Colorado 80528-9599

PATENT APPLICATION

ATTORNEY DOCKET NO. 10992668-1

IN THE U.S. PATENT AND TRADEMARK OFFICE
Patent Application Transmittal LetterASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 CFR 1.53(b) is a(n): ☒ Utility ☐ Design☒ original patent application,☐ continuation-in-part application

INVENTOR(S): Slawomir K. Ilnicki, et al.

TITLE: Secure Data Transfer Method And System

Enclosed are:

☒ The Declaration and Power of Attorney. ☒ signed ☐ unsigned or partially signed☒ 8 sheets of drawings (one set) ☐ Associate Power of Attorney☐ Form PTO-1449 ☐ Information Disclosure Statement and Form PTO-1449☐ Priority document(s) ☐ (Other) (fee \$)

CLAIMS AS FILED BY OTHER THAN A SMALL ENTITY				
(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) TOTALS
TOTAL CLAIMS	19 — 20	0	X \$18	\$ 0
INDEPENDENT CLAIMS	4 — 3	1	X \$78	\$ 78
ANY MULTIPLE DEPENDENT CLAIMS	0		\$260	\$ 0
BASIC FEE: Design \$310.00); Utility \$690.00)				\$ 690
TOTAL FILING FEE				\$ 768
OTHER FEES				\$
TOTAL CHARGES TO DEPOSIT ACCOUNT				\$ 768

Charge \$ 768 to Deposit Account 08-2025. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16, 1.17, 1.19, 1.20 and 1.21. A duplicate copy of this sheet is enclosed.

"Express Mail" label no. EL519584483USDate of Deposit June 13, 2000

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

By Tiffany Turner

Typed Name: Tiffany Turner

Respectfully submitted,

Slawomir K. Ilnicki, et al.

By Thomas Li

Thomas Li

Attorney/Agent for Applicant(s)

Reg. No. 37,079

Date: June 13, 2000

Telephone No.: (650) 857-5972

United States Patent Application
For

SECURE DATA TRANSFER METHOD AND SYSTEM

Inventors:

Slawomir Ilnicki
Troy Shahoumian

EXPRESS MAIL CERTIFICATE OF MAILING

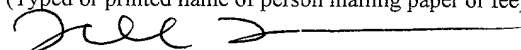
"Express Mail" mailing label number: **EL519584483US**

Date of Deposit: **June 13, 2000**

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

TIFFANY TURNER

(Typed or printed name of person mailing paper or fee)



(Signature of person mailing paper or fee)

SECURE DATA TRANSFER METHOD AND SYSTEM

Field of the invention

The present invention relates generally to data security systems and more specifically to a method and system for securely sending data between an agent in a non-secure (e.g., hostile) environment and a server behind a firewall.

Background of the Invention

DATA COLLECTION APPLICATION

As an increasing number of businesses offer products and services via the Internet on the World Wide Web (WWW), there is a corresponding need by the businesses for feedback mechanisms to inform the businesses regarding how quickly information requested by users or clients are actually provided. One such feedback mechanism is a data collection application. The data collection application measuring the amount of time it takes for a particular Web page to load in a user's browser. As can be appreciated, the user's view (i.e., the time delay actually experienced by the user) is the most accurate indicator of a particular Web site's performance. In order to obtain a user's view, it is necessary to have an agent that resides at the user's browser. The agent can then record the time delay experienced by the user for a particular web page or other information to be displayed or loaded. The time delay is simply the time that elapses from the time a request (e.g., HTTP request) is initiated by a user selecting a particular link to the time that the Web page is loaded into the user's browser program.

One area where such an application would find use is in on-line brokerage services for the trading of securities. As an on-line brokerage service provider, the business would like to have a mechanism that would differentiate between its users and provide a higher level of service to those customers that have shown themselves to be worthy of a higher level of service. For example, it would be desirable for a business owner to efficiently allocate a more responsive service (e.g., a quicker and more timely connection) to certain clients that meet a predetermined criteria (e.g., length of business relationship, volume of business, etc.).

A data collection application is a key piece in a solution to provide differing levels of service to different users based on predetermined criteria. The data collection (also referred to as a "measuring application") sends measuring agents to the different users. Each of the measuring agents send time stamped information regarding the length of time needed to retrieve pages,

download information, receive data, etc. from the user where the agent is located. This time information can be utilized by the data collection application or by another application to allocate resources. Perhaps, if a connection with a "good" client is very poor, a new connection can be utilized for that client or bandwidth can be allocated in some other way to that client. On the other hand, if it is detected that a user, who is not yet a client and simply exploring the web site, has a very fast connection, a slower connection can be allocated thereto. Accordingly, the business owner can provide service to all its users, but has a mechanism by which it can efficiently allocate a more responsive service (e.g., a quicker and more timely connection) to certain clients that meet a predetermined criteria (e.g., length of business relationship, volume of business, etc.).

As can be appreciated, in such a system it is important to the user that the code (e.g., agent) is from a trusted source. For example, if the code is from an impostor, the code can include a malicious virus that destroys or corrupts the user's data or even sends sensitive information to the impostor.

Similarly, it is important to the business owner that the agent is code that was planted by the owner and not code (e.g., agent) written by a non-trusted third party. For example, if a user discovers how the agent operates and changes the code in the agent, the user can deceive the measuring agent into thinking (1) the performance is very poor when in fact the performance is very good; and/or (2) that the client's behavior or traits deserve a higher level of service where in fact the client's actual behavior or traits are not deserving of a higher level of service. In so doing, the third party would defraud the measuring application in order to obtain a high level of service. Accordingly, it is important to have a security mechanism that assures the user that the measuring agent is from a trusted source (e.g., the brokerage service provider). In addition, it is important to have a mechanism to assure the data collection application that information received from the agent is provided by the true agent and not a foreign code that is generated by a hacker.

There are two security approaches to this problem: (1) placing the web server and the data collection application in the same security zone; and (2) placing the web server and the data collection application in different security zones. As described hereinafter, both approaches offer only tolerable solutions that each has different disadvantages and exposure to different security threats.

WEB SERVER AND APPLICATION IN THE SAME SECURITY ZONE

In this approach, the web server and the application must run in the same security perimeter or zone. The security zone can be protected or not protected by a firewall. For example, when an Internet Service Provider (ISP) is hosting the web server, then the application
5 must also run at the ISP site. Running the application at the ISP site may not be desirable for security reasons.

The security zone can also be behind a firewall. FIG. 1 illustrates a block diagram of a case where both the application and the web server reside in a security zone that is behind a firewall. A measuring agent 4 resides in a browser 8. A web server 12 and application
10 measuring server 16 reside in a security zone 20 behind a firewall 24. The measuring agent 4 communicates data to the web server 12 through a secure channel (e.g., a secure socket layer protocol (SSL)). It is noted that the secure HTTP/SSL link passes through the firewall 24. The web server 12 then receives the data and sends the data to a common gateway interface (CGI)
15 script 28 through a first pipe 32. In turn the (CGI) script 28 sends the data to the application measuring server 16 through a second pipe 36.

Unfortunately, attacks on web servers are notorious, and breaches in web server security occur very often. Consequently, putting a web server 12 behind the firewall 24 exposes the system behind the firewall 24 to numerous types of attacks. For example, if the web server 12
20 begins to malfunction either due to internal problems or by malicious attacks (e.g., through malformed URLs), an intruder may gain access to privileges that can allow the intruder to wreck havoc and cause much damage to the system.

Therefore, web servers that are externally visible to users are typically not placed in the same trusted environment as other mission critical resources or confidential and sensitive data. Instead, these web servers are often hosted by third parties, such as Internet Service Providers,
25 and web applications that operate on confidential data are within their own trusted security zone (e.g., behind their own firewall). In other words, the vulnerability of web servers causes the placement of externally visible web servers in non-trusted or semi-trusted (e.g., a de-militarized zone) rather than in a trusted environment (e.g., behind a firewall) where mission critical applications and confidential data reside.

WEB SERVER AND APPLICATION IN DIFFERENT SECURITY ZONES

FIG. 2 illustrates a block diagram of a second conventional approach for sending data. In this approach the web server and the application reside in different security zones. Those elements that are the same as in FIG. 1 are labeled with the same numeral. It is noted that this approach is more widely utilized because of the threats and exposure, discussed previously, of sensitive data when the web server and the application reside in the same security zones.

A measuring agent 4 resides in a browser 8 as in the case of the system of FIG. 1. An application measuring server 16 resides in a security zone 20 behind a firewall 24. A web server 12 resides in a second security zone 40. The measuring agent 4 communicates data to the web server 12 through a secure channel (e.g., a secure socket layer protocol (SSL)). The web server 12 then receives the data and sends the data to a common gateway interface (CGI) script 44 through a first pipe 48. In turn the (CGI) script 44 sends the data to the application measuring server 16. The script 44 can use a second secure channel (e.g., SSL connection, secure shell (SSH) or a virtual private network (VPN), etc.) to protect the data when crossing the firewall 24.

Unfortunately, this approach suffers from several disadvantages. First, the data being transmitted is exposed at the web server 12. Consequently, if someone breaches the security of the web server 12, the confidential data may be intercepted and used for purposes other than the intended purpose.

Second, there are problems associated with how the communication is established between the web server 12 and the application 16 running behind the firewall. Typically, a CGI script running on behalf of the web server 12 initiates the TCP/IP connection to the measurement application server 16 and operates in a "push" mode. This type of connection is referred to as the "push" mode because data is pushed from the web server 12 to the measurement application server 16 behind the firewall 24. Unfortunately, most firewall security policies do not allow TCP/IP connections that originate from outside the firewall 24. The rationale for this policy is to protect against malicious attacks through such connections. These malicious attacks may be in the form of a denial of service attacks, breaking an application functionality, exploring application weaknesses, or obtaining privileges that allow for penetration of systems behind the firewall 24.

One can change a firewall's security policy to allow incoming TCP/IP connections. However, changing a firewall's open IP addresses and ports is considered to be an extremely

5

Accordingly, there remains a need for a method and system for securely transferring data between an agent in a non-secure environment and a server behind a firewall that overcomes the disadvantages set forth previously.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method for passing data efficiently from an agent in a non-secure (e.g., hostile) environment to an application server behind a firewall without requiring a trusted intermediate party (e.g., a web server or secure channels).

5 It is a further object of the present invention to provide a method for passing data efficiently from an agent in a non-secure (e.g., hostile) environment to an application server behind a firewall without requiring the firewall to open to incoming TCP/IP connections.

10 It is yet another object of the present invention to provide a method for passing data efficiently from an agent in a non-secure environment to an application server behind a firewall without requiring the security policies of firewalls to be weakened.

15 A method and system for securely transferring data between an application server and an agent of the application server through a non-trusted node. First, a public key of the application server is embedded in the code of the agent so that verification of the signature of the agent code implicitly authenticates the public key of the application server. Next, a communication link is established between the application server and the non-trusted node through a relay module.

20 Verification of the signature of the agent signature also provides authentication of the embedded public key of the application server since the public key is part of the downloaded and signed code. In other words, if the user trusts the code, the user also trusts the embedded public key. By embedding the public key in the agent code, the present invention allows for implicit authentication of the public key when the code itself is authenticated (e.g., when the code is signed by a trusted authority).

25 The agent in turn can use the public key to transfer a secret session key that is utilized to encrypt data that is to be sent to the application server. Since only the owner of the private key associated with the public key can retrieve the session key used for data encryption, should the encrypted data be hi-jacked at the non-trusted node, the hi-jacker cannot recover the information. In addition, it is the application server that initiates the TCP/IP connection with the relay module.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements.

FIG. 1 illustrates a block diagram of a first conventional approach for sending data.

FIG. 2 illustrates a block diagram of a second conventional approach for sending data.

FIG. 3 is a flowchart illustrating the method of one embodiment of the present invention.

FIG. 4 is a diagram illustrating the steps for establishing a session key between the measuring agent and the measuring server in accordance with one embodiment of the present invention.

FIG. 5 illustrates a block diagram of a system for securely transferring data that is configured according to one embodiment of the present invention.

FIG. 6 is a diagram illustrating the steps for establishing a connection between the measuring server and the relay module in accordance with one embodiment of the present invention.

FIG. 7 is a flowchart illustrating the steps performed by the measuring agent of FIG. 5 according to one embodiment of the present invention.

FIG. 8 is a flowchart illustrating the steps performed by the measuring server of FIG. 5 of one embodiment of the present invention.

FIG. 9 is a flowchart illustrating the steps performed by the instantiation module of FIG. 5 of one embodiment of the present invention.

FIG. 10 is a flowchart illustrating the steps performed by the relay module of FIG. 5 of one embodiment of the present invention.

FIG. 11 is a flowchart illustrating the steps performed by the forwarding module of FIG. 5 of one embodiment of the present invention.

DETAILED DESCRIPTION

In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention. The following description and the drawings are illustrative of the invention and are not to be construed as limiting the invention.

Secure Data Transfer System 500

FIG. 5 illustrates a block diagram of a system 500 for securely transferring data that is configured according to one embodiment of the present invention. The system 500 includes a first security zone 520 that is behind a firewall 528. A measuring application server program 524 can reside in the first secure zone 520. The programs that are external to the first security zone 520 (i.e., not disposed behind the firewall 528) are considered to be in a non-trusted or non-secure environment (also referred to herein as a hostile environment).

The system 500 also includes a browser program 510 (e.g., a Netscape Communicator browser program or a Windows Internet Explorer browser program) that typically resides on a user's personal computer (PC), and one or more intermediate nodes (e.g., node 530) between the browser program 510 and the application measuring server 524. The browser 510 can download a measuring agent 514 in accordance with steps 400 and 404, which are described in greater detail with reference to FIG. 4.

The intermediate node 530 can be an Internet Service Provider (ISP) web server node for providing Internet access services. Preferably, several key components of the present invention are disposed in the intermediate node 530 that may be a non-secure node.

The present invention provides an end-to-end secure communication link between an agent 514 and an application server 524 even though there is a non-trusted intermediate node therebetween. A secure transfer module 548 of the present invention includes an instantiation module 550, a relay module 560, and optionally a forwarding module 570. The relay module 560 includes a first port 561 for connecting to the forwarding module 570 and a second port 562 for connecting to the application measuring server 524.

The instantiation module 550 specifies a specific port number for the first port 561 and another specific port number for the second port 562 and provides the port numbers to the relay module 560. In turn, the relay module 560 listens on the specified ports. For example, the relay module 560 waits for the measuring application server program to initiate connection to the second port 562 at the specified port number. It is noted that the relay module 560 does not establish the connection with the application measuring server 524, but waits for the application measuring server 524 to make the connection, thereby not requiring any changes to existing security policies of firewall 528.

The instantiation module 550 loads and runs the relay module 560. If a copy of the relay module 560 does not reside on the web server node 530, the instantiation module 550 can download a copy of the relay module from another server and install the copy on the web server 540. The forwarding module 570 is optionally provided to forward data from the measuring agent 514 to the relay module 560 when the connection between the browser 510 and the web server 540 is HTTP based. It is noted that the instantiation module 550 is not needed if a Java applet or an Active X is establishing a direct connection with the relay module 560.

Modules 550, 560, and 570 can be implemented with programming instructions, such as CGI scripts, to perform the steps illustrated in FIGS. 9-11, respectively. The modules 550, 560, and 570 are described in greater detail hereinafter with reference to FIGS. 9 to 11.

End-to-End Secure Communication between Browser Client and Application server

FIG. 3 is a diagram illustrating the method of establishing an end-to-end secure communication between a data collecting agent and a data collecting application server in accordance with one embodiment of the present invention. In step 304, a secret key is established (e.g., shared) between the browser client and the application server by utilizing a public key of the application server that is embedded into the agent. In step 308, a connection is established between an intermediate node (e.g., a web server) and the application server by utilizing a relay module that opens a socket, listens on a specified port on the socket, and waits for the application server to make a connection to the specified port. In step 314, data is transferred between the agent and the application server by utilizing the connection established through the relay module.

Establishing a Session Key

FIG. 4 is a diagram illustrating the steps for establishing a session key between the measuring agent and the measuring server in accordance with one embodiment of the present invention. In step 400, a user downloads the measuring agent 514 that includes the public key of the measuring applicat on server program 524. For example, the public key can be appended to, attached to, or embedded in the agent 514, or included in the agent 514 by using some other manner.

In step 404, a user accepts a signed measuring agent code 514 and authenticates the origin of the measuring agent 514 using standard browser verification methods. One aspect of the present invention is including the public key of the measuring server 524 in the measuring agent 514. By so doing, the public key of the measuring server 524 can be conveniently authenticated (i.e., implicitly authenticated) when the user authenticates the agent code. This implicit authentication obviates the need for a user to connect to a certification authority to verify the public key of the measuring server 524.

In step 408, the browser 510 launches the measuring agent 514. In this step, a secret key is established to encrypt and decrypt data to be transmitted between the agent 514 and the measuring application server 524. The secret key can be established by either a key agreement protocol or a key transfer protocol. In a key agreement protocol (e.g., a Diffie-Hellman (DH) public key algorithm), either party can derive the shared secret key based on the other party's public key. In a key transfer protocol (e.g., a RSA public key algorithm), the shared secret key is generated by one party (e.g., by the measuring agent 514), encrypted with the other party's public key (e.g., by the public key of the measuring application server 524), and then transferred to the other party.

In step 418, the measuring application 524 retrieves or derives the shared secret key by utilizing its own private key depending on the method used to establish the secret key.

When authentication of the system that hosts the measuring agent 514 is needed or when the Diffie-Hellman (DH) public key algorithm is used to establish a shared secret key between the measuring agent 514 and the measuring application 524, an end-to-end secure channel (e.g., a channel between the agent 514 and the web server 540) can be utilized to protect the integrity of the public key of the measuring agent 514 if the public key is not certified or encrypted by the shared secret key. The application measuring server program 524 can retrieve the public key of

the measuring agent 514 from the web server 540 by also using a secure channel.

A challenge-response protocol, which is well known by those of ordinary skill in the art, can be utilized, and a certificate for the public key of the measuring agent 514 can be required in order to authenticate the measuring agent 514 and to prevent man-in-the-middle attacks. The secure end-to-end communication protocol of the present invention preferably utilizes sequence number in order to prevent replay attacks. Furthermore, a standard encryption algorithm can be utilized to increase confidentiality, and a fast hashing algorithm (e.g., Keyed-Hashing for Message Authentication (HMAC) - IETF RFC 2104) to increase message data integrity and authentication.

Establishing A Connection Between The Measuring Server 524 And The Relay Module
560

FIG. 6 is a diagram illustrating the steps for establishing a connection between the measuring server and the relay module in accordance with one embodiment of the present invention. In step 604, the measuring application server program 524 runs the instantiation module 550 in response to a request to the web server 540. The web server 540 in turn runs the instantiation module 550 (e.g., a CGI script). The instantiation module 550 retrieves from the application measuring server 524 the specific port on which to listen for incoming connection from the application measuring server 524 and the specific port on which to connect to the forwarding module 570. The instantiation module 550 can also retrieve the name of the relay module 560 and run the relay module 560.

In one embodiment, the relay module 560 creates a first port (e.g., a TCP/IP socket) on the specified port number and listens for an incoming TCP/IP connection on the specified port. Once the first socket is successfully created, the control returns to the measuring application server 524. The measuring application server program 524 then initiates a TCP/IP connection to the relay module 560 using the open TCP/IP socket. In addition, the relay module 560 creates a port (e.g., a TCP/IP socket) on the specified port number on which to listen for incoming traffic from the forwarding module 570. The specific port numbers are parameters that are passed from the instantiation module 550 to the relay module 560. The steps performed by the instantiation module 550 in accordance with one embodiment of the present invention are described in greater detail hereinafter with reference to FIG. 9.

Alternatively, the connection between the relay module 560 and the measuring application server 524 can be established via electronic mail. This alternative is especially useful for those firewalls that do not allow any other types of TCP/IP connections (incoming or outgoing). Since regular electronic mail is universally accepted as a communication channel, most firewalls allow for incoming e-mail.

In step 608, the instantiation module 550 starts the relay module 560 that listens to the specified port. The steps performed by the relay module 560 in accordance with one embodiment of the present invention are described in greater detail hereinafter with reference to FIG. 9.

In step 614, the measuring application server program 524 connects to the relay module 560 at the specified port. Certain firewall configurations require special instructions to allow outgoing TCP/IP connections. In such cases, a standard SOCKS proxy, which can running on the firewall 528, can be utilized to accomplish "sockification" of the measuring application server program 524. "Sockification" links the measuring application 524 with a SOCKS library in order to run a SOCKS protocol on top of a TCP/IP connection.

In step 620, the browser 510 loads the measuring agent 514. In step 624, the measuring agent 514 and the measuring application server 524 establish a secret key. It is noted that steps 620 and 624 can occur anytime prior to step 630.

In step 630, the measuring agent 514 encrypts the data using the secret key and sends the encrypted data over a connection (e.g., an HTTP connection) to the web server 540. In step 640, the web server 540 cooperates with the forwarding module 570 to send the data to the relay module 560 over a predetermined pipe or port. Preferably a pipe is utilized for process to process communication within the same system. When a TCP/IP protocol is used, ports are utilized. It is noted that on the same machine, the use of a pipe can be more efficient and use fewer resources. The steps performed by the forwarding module 570 in accordance with one embodiment of the present invention are described in greater detail hereinafter with reference to FIG. 9.

In step 650, the relay module 560 pushes the data received from the forwarding module 570 over the previously established connected (e.g., a previously established TCP/IP connection or an HTTP connector). Furthermore, the relay module 560 can also pull information from the measuring server 524 (e.g., re-configuration parameters) and pass this information to the agent 514 via the forwarding module 570. Accordingly, the present invention provides a bi-directional

end-to-end secure communication link between the agent 514 and the measuring server 524. It is noted that in this example, since HTTP is a request/reply protocol between the measuring agent 514 and the measuring server 524, the measuring server 524 can only push information to the agent 514 as a reply to the agent request (e.g., the HTTP request). However, in other non-request/reply protocols, the measuring server 524 can push information to the agent 514.

Measuring Agent 514

FIG. 7 is a flowchart illustrating the steps performed by the measuring agent 514 of FIG. 5 according to one embodiment of the present invention. In step 704, when a key transfer protocol (e.g., RSA algorithm) is utilized, the measuring agent 514 generates a session key (e.g., a secret key). This step can be omitted in a key agreement protocol (e.g., Diffie-Hellman public key algorithm) where the measuring server 524 can independently derive the session key by utilizing the other party's public key.

In step 708, the measuring agent 514 encrypts the session key by using the measurement server's public key. It is noted that the measurement server's public key does not need to be verified because it is embedded as part of the measurement agent's code, whose signature the user verified through the browser program when the measuring agent code is initially downloaded.

In step 714, the measuring agent 514 collects data. In step 718, the measuring agent 514 encrypts the data collected in step 714 using the session key. In step 724, the measuring agent 514 sends the encrypted data to the measurement server via a non-trusted intermediate node (e.g., the web server node 530). In step 724, the measuring agent 514 can also include (e.g., append) the encrypted session key (i.e., the session key encrypted with the measuring server's public key) with the encrypted data under certain circumstances. These circumstances can include (1) if this is the first time data is being transmitted to the measuring server 524 or (2) if the session key has to change for some reason, such as, to adhere to predetermined security policies.

In step 728, the measuring agent 514 determines if the measuring server 524 has sent any data for the measuring agent 514 to receive. If no, processing continues at processing step 714. If yes, the measuring agent 514 decrypts the received data (e.g., configuration data) and processes the data in step 734.

Measuring Server 524

FIG. 8 is a flowchart illustrating the steps performed by the measuring server 524 of FIG. 5 of one embodiment of the present invention. In step 804, the measuring server 524 instantiates the relay module 560 by contacting the web server 540 and providing the URL of the relay module 560 with three parameters: (1) the program name of the relay module; (2) a port number for the first port 561; and (3) a port number of the second port 562.

In step 808, the measuring server 524 connects to the relay module 560 that is listening on the specified port number at the second port 562. In step 814, the measuring server 524 reads data through the connected with the relay module 560. In step 818, a determination is made whether the encrypted session key is included in the received data. If yes, in step 824, the measuring server 524 decrypts the encrypted session key by utilizing the private key of the measuring server 524.

If no, in step 828, the measuring server 524 sends information to the measuring agent 514 via the connection to the relay module 560 (e.g., by writing the data to the connection). For example, this information can be an acknowledgment (ACK) that data from the agent has been received or other data for the agent (e.g., configuration data) encrypted with the session key.

In step 834, the measuring server 524 decrypts the data received in 814 by utilizing the session key. In step 838, the measuring server 524 processes the data decrypted in step 834.

Instantiation Module 550

FIG. 9 is a flowchart illustrating the steps performed by the instantiation module 550 of FIG. 5 of one embodiment of the present invention. In step 904, the instantiation module 550 extracts the program name of the relay module, the port number for the first port 561 and the port number for the second port 562 from the URL request of the measuring server 524. In step 908, the instantiation module 550 executes the relay module 560 with two parameters: (1) the port number for the first port 561 and (2) the port number for the second port 562. As described earlier, the first port 561 listens for incoming connection from the forwarding module and the second port 562 listens for incoming connection from the measurement server 524.

Relay Module 560

FIG. 10 is a flowchart illustrating the steps performed by the relay module 560 of FIG. 5 of one embodiment of the present invention. In step 1004, the relay module 560 receives the two

port numbers for the first 561 and second port 562, respectively as input parameters set by the instantiation module 550. In step 1008, the relay module listens on the second port for a connection from the measurement server 524. Preferably, this connection remains open. In step 1014, the relay module 560 connects to the forwarding module 570 on the first port 561. In step 1018, the relay module 560 reads data on the first port 561 from the forwarding module 570. In step 1024, the relay module 560 writes data on the second port 562 to the measurement server 524. In step 1028, the relay module 560 reads data on the second port 561 from the measurement server 524. In step 1034, a determination is made whether data is received. If yes, in step 1038, the relay module 560 writes data on the first port 561 to the forwarding module 570. If no, in step 1044, the relay module 560 disconnects from the first port 561 and the forwarding module 570.

Forwarding Module 570

FIG. 11 is a flowchart illustrating the steps performed by the forwarding module 570 of FIG. 5 of one embodiment of the present invention. In step 1104, the forwarding module 570 connects to the first port 561 of the relay module 560. This step may be triggered by the URL request of the measuring agent 514. In step 1108, a determination is made whether a connection has been successfully established. If yes, in step 1114, the forwarding module 570 extracts data from the URL request sent by the measuring agent 514. If no, in step 1138, the forwarding module 570 sends a "Cannot Transfer Data" message back to the measuring agent 514 via the Web server 540 and exits.

In step 1118, the forwarding module 570 writes data on the open connection to the relay module 560. In step 1124, the forwarding module 570 waits for an acknowledgment (ACK) and optional reply data (e.g., re-configuration information) from the measuring server 524.

In step 1128, a determination is made whether a reply data has been received. If the reply data has been received, then in step 1134 the forwarding module 570 transfers the received reply data to the measuring agent 514 via the web server 540. If no, the processing skips step 1134 and exits.

It is noted that the principles of the present invention has been described in connection with an example that includes a data collecting agent and a corresponding data collecting server.

However, the teachings of the present invention can be applied to other applications and other situations whenever there is a need to transfer data from an application in a non-secure environment to a server in a trusted security zone or trusted environment. A non-secure (e.g., hostile) environment can be any environment (e.g., a non-trusted environment or semi-trusted environment) that is separate from an environment where mission critical applications and confidential data reside. The trusted environment can be the security zone behind a firewall.

Accordingly, a method and system for passing data efficiently between an agent in a hostile environment to a application server behind a firewall without requiring a trusted intermediate party (e.g., a web server or secure channels) has been described.

One advantage of the present invention is the provision of end-to-end security not merely a point-to-point security. By providing end-to-end security, the relay module 560 or any module running as part of the intermediate node 530 (e.g., a web server node or environment) does not have to be trusted. For example, if the encrypted data is hijacked at the intermediate node 530, the encrypted data is not exposed since the hijacker cannot recover the data without the application server's private key.

Another advantage of the present invention is that by embedding the public key of the application server in the agent code, the public key is implicitly authenticated when the user verifies the signature of the agent code. Accordingly, the present invention obviates the need for and attendant complexities (e.g., cumbersome procedure for determining a source for the public key, accessing a certification authority, etc.) involved in the explicit authentication of the public key, thereby saving time and simplifying the process for the user.

A further advantage of the present invention is that it does not weaken the existing security infrastructure. For example, the present invention does not require a firewall to make exceptions to its security policies by accepting incoming connections through the firewall.

Another advantage of the present invention is that it is non-intrusive to the client browser and the web server. Regarding the client browser, the agent code that incorporates the public key of the application server is downloaded using standard procedures for downloading any application without need for further configuration or plug-in applications. Regarding the web server, the present invention can be implemented as CGI scripts that are uploaded in the usual fashion to a CGI bin directory for subsequent access by the web server.

The foregoing description has provided numerous examples of the present invention. It will be appreciated that various modifications and changes may be made thereto without departing from the broader scope of the invention as set forth in the appended claims.

CLAIMS

What is claimed is:

1. A method for securely transferring data between an agent and an application server through a non-secure node comprising:
 - (a) establishing a session key between the agent and the application server by utilizing a public key of the application server; wherein the public key of the application server is embedded in the agent; and
 - (b) establishing an end-to-end secure connection between the agent and the application server by using the session key and by establishing a communication link between the application server and the non-secure node by using a relay module.
2. The method of claim 1 wherein establishing a communication link between the application server and the non-secure node by using a relay module comprises:
 - dynamically instantiating the relay module having a first port for communicating with the application server and a second port for communicating with the agent, the relay module listening on a first predetermined port number on the first port and a second predetermined port number on the second port; and
 - the application server connecting to the first port of the relay module to establish a connection therewith.
3. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:
 - pushing data encrypted by the established session key from the agent to the application server over the end-to-end secure connection.
4. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:

pulling data encrypted by the session key from the application server over the end-to-end secure connection to the agent.

5. The method of claim 1 wherein establishing a session key between the agent and the application server by utilizing a public key of the application server further comprises:

establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween.

6. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween comprises:

encrypting the shared secret key with the public key of the application server to generate an encrypted shared key;

sending the encrypted shared secret key to the application server; and

decrypting the shared secret key with the private key of the application server.

7. The method of claim 5 wherein establishing a shared secret key between the application server and the agent utilizes a key transfer protocol.

8. The method of claim 7 wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm.

9. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween utilizes a key agreement protocol.

10. The method of claim 9 wherein the key agreement protocol is the Diffie-Hellman (DH) public key algorithm.

11. The method of securely transferring data between an application server and an agent of the application server through a non-secure environment having a web-server and the agent, the method comprising:

- a) a user accessing the web-server to download the agent therefrom; wherein the agent includes a public key of the application server;
- b) the agent establishing a shared session key with the application server by using the public key of the application server, the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server;
- c) the application server establishing a connection to the web-server; and
- d) the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server.

12. The method of claim 11 wherein the application server establishing a connection to the web-server further comprises

- c1) the application server dynamically instantiating a relay module by sending a URL associated with the relay module to the web-server, the URL specifying a first predetermined port for communication between the web-server and the relay module;
- c2) the application server connecting to the relay module on a first predetermined port; and
- c3) the application server reading data from the relay module through the connection on the first predetermined port.

13. The method of claim 12 wherein the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server further comprises

- d1) the agent encrypting the session key with the public key of the application server;
- d2) the agent collecting data;
- d3) the agent encrypting the collected data with the session key;
- d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module.

14. The method of claim 11 wherein the first protocol is one of HTTP and HTTP/SSL.

15. A secure data transfer system for connecting a non-secure node to an application server behind a firewall comprising:

- a) a web-server in the non-secure node;
- b) a relay in the non-secure node that is dynamically instantiated by the application server, the relay having a first port for listening for a connection from the application server;

wherein the application server connects to the relay on the first port and reads data from the first port.

16. The secure data transfer system of claim 15 further comprising:

- a) an instantiation module for instantiating the relay module in response to an URL associated with the relay module.

17. A secure data transfer system for establishing an end-to-end secure connection between an agent and an application server behind a firewall through a non-secure node comprising:

- a) a web-server residing in the non-secure node, the web-server having the agent that includes a public key of the application server;

- b) a browser in communication with the web-server for downloading the agent from the web-server;
- c) a secure transfer module residing in the non-secure node; and
- d) an application server in a secure zone for initiating a connection to the web-server via the secure transfer module.

18. The secure data transfer system of claim 17 wherein the secure transfer module further comprises:

- c1) a relay module for listening to a first port and a second port;
 - c2) an instantiation module for executing the relay module in response to a command from the application server;
 - c3) a forwarding module for transferring data from the agent to the relay module in response to a command from the agent; and
- wherein the relay module listens to the first port for a connection by the application server and listens to the second port for a connection by the forwarding module.

19. The secure data transfer system of claim 16 wherein the non-secure node is a web-server node.

ABSTRACT OF THE DISCLOSURE

A method and system for securely transferring data between an application server and an agent of the application server through a non-secure node. First, a session key between the agent and the application server is established by utilizing a public key of the application server that is embedded in the code of the agent. Next, an end-to-end secure connection is established between the agent and the application server by using the session key and by establishing a communication link between the application server and the non-secure node by using a relay module.

09593322, 03.1.2009

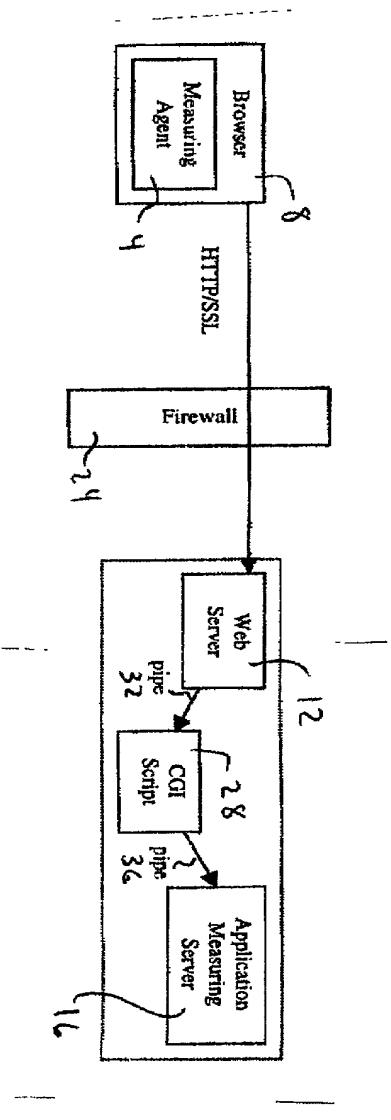


FIG. 1 (PRIOR ART)

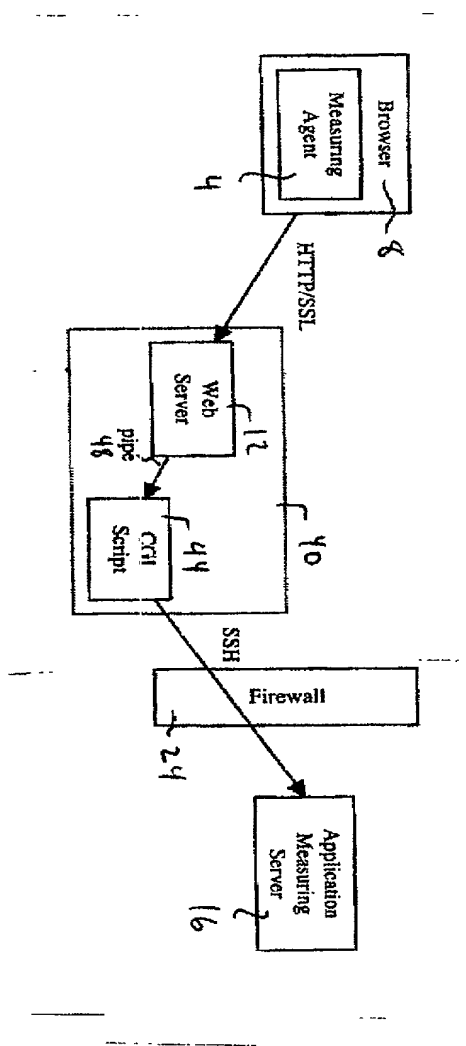


FIG. 2 (PRIOR ART)

```

graph TD
    A[ESTABLISH A SESSION KEY  
BETWEEN THE SERVER APPLICATION  
AND THE AGENT] --> B[ESTABLISH A CONNECTION  
BETWEEN THE SERVER APPLICATION  
AND AN INTERMEDIATE  
NODE (E.G., A WEB SERVER) VIA  
A RELAY MODULE]
    B --> C[TRANSFER DATA BETWEEN THE  
AGENT & SERVER APPLICATION  
THROUGH THE RELAY]
  
```

ESTABLISH A SESSION KEY
BETWEEN THE SERVER APPLICATION
AND THE AGENT 304

ESTABLISH A CONNECTION
BETWEEN THE SERVER APPLICATION
AND AN INTERMEDIATE
NODE (E.G., A WEB SERVER) VIA
A RELAY MODULE 308

TRANSFER DATA BETWEEN THE
AGENT & SERVER APPLICATION
THROUGH THE RELAY 314

Browse	Agent	Web Server	Measuring Server Application
User accepts signed agent and at the same token authenticates its origin. 404	User downloads agent with apps public key 400 Browser launches agent Agent derives shared secret from its and apps public keys (DH) 408		
	Agent sends its public key 414		Application derives shared secret from browser/agent public key and its own (DH). 418

FIG. 4

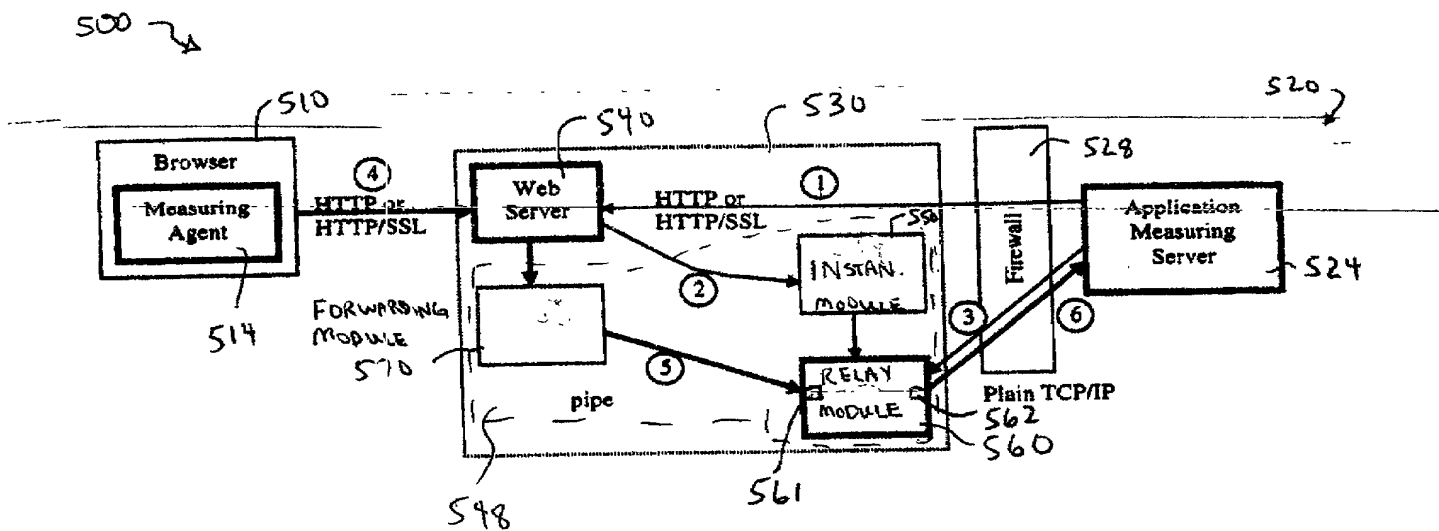


FIG. 5

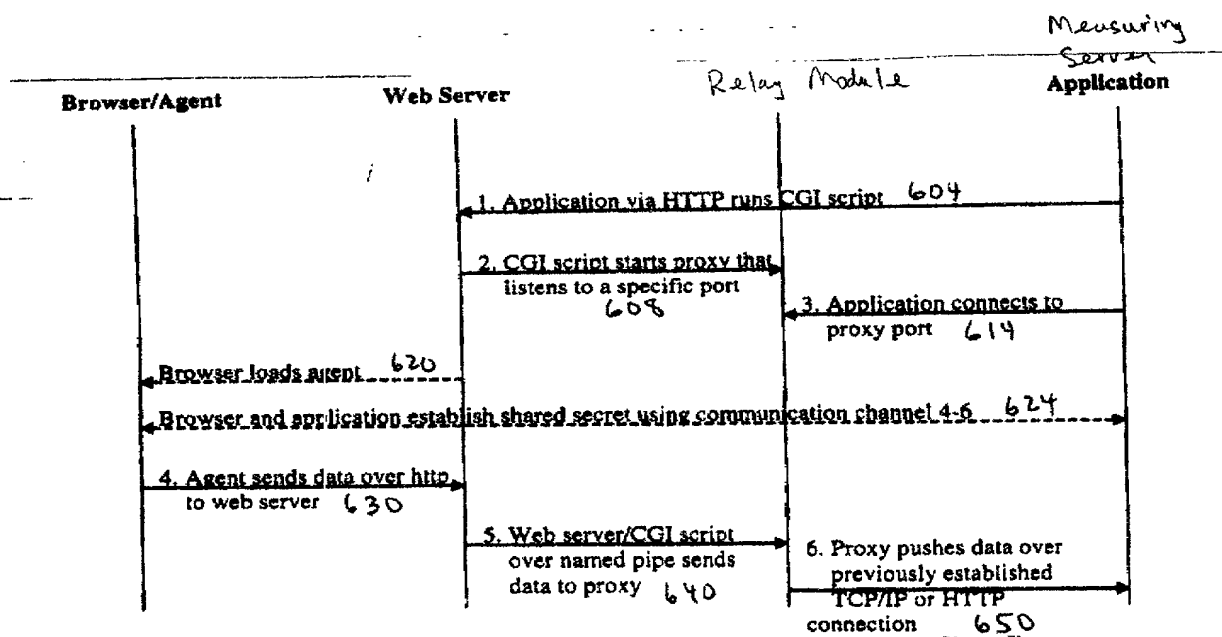


FIG. 6

```
graph TD; Start([Start]) --> 704[Generate session (secret) key (if RSA alg is used to transfer session key)]; 704 --> 708[Encrypt session key using Application Measurement Server public key (RSA alg).  
Note: the Application Measurement Server key does not have to be verified because it is a part of the agent code that the user (via a browser) verified signature when the agent code was downloaded]; 708 --> 714[Collect measured data]; 714 --> 718[Encrypt measured data using session (secret) key]; 718 --> 724[Send encrypted measured data and encrypted session key to the Application Measurement Server via web serve.  
Note: the encrypted session key has to be appended to the encrypted data if: (1) if this is the first time data is sent or (2) if the session key has to change (security policy may require changing session key from time to time)]; 724 --> 728{Receive data?}; 728 -- No --> 728; 728 -- Yes --> 734[Decrypt received data (e.g., configuration data) and process it.]; 734 --> End([End]);
```

The flowchart illustrates a secure data transfer process. It begins with a 'Start' terminal, leading to step 704: 'Generate session (secret) key (if RSA alg is used to transfer session key)'. This is followed by step 708: 'Encrypt session key using Application Measurement Server public key (RSA alg).', which includes a note that the server's key does not need verification as it is part of the agent code verified by the user. The process then moves to step 714: 'Collect measured data', followed by step 718: 'Encrypt measured data using session (secret) key'. Step 724 involves 'Send encrypted measured data and encrypted session key to the Application Measurement Server via web serve.', with a note about appending the session key under specific conditions. A decision diamond at step 728 asks 'Receive data?'. If 'No', it loops back to 724. If 'Yes', it proceeds to step 734: 'Decrypt received data (e.g., configuration data) and process it.', which then leads to an 'End' terminal.

FIG. 7

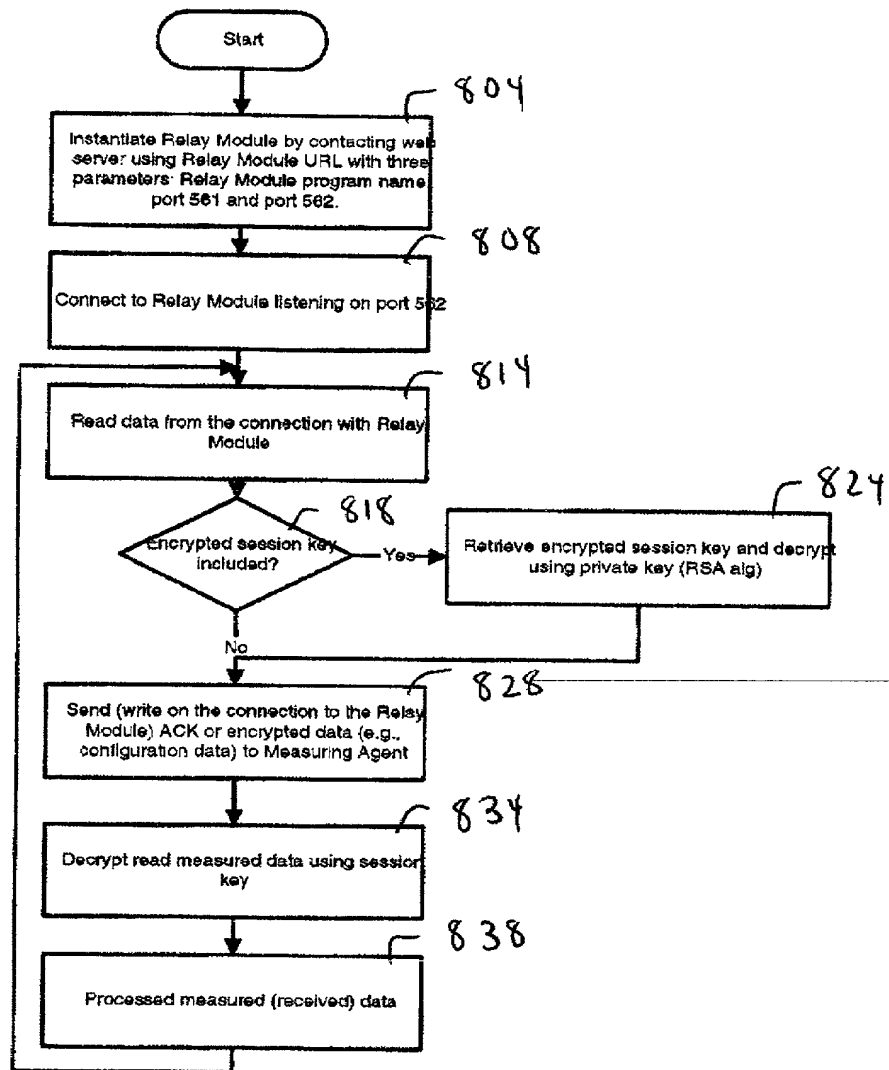


FIG. 8

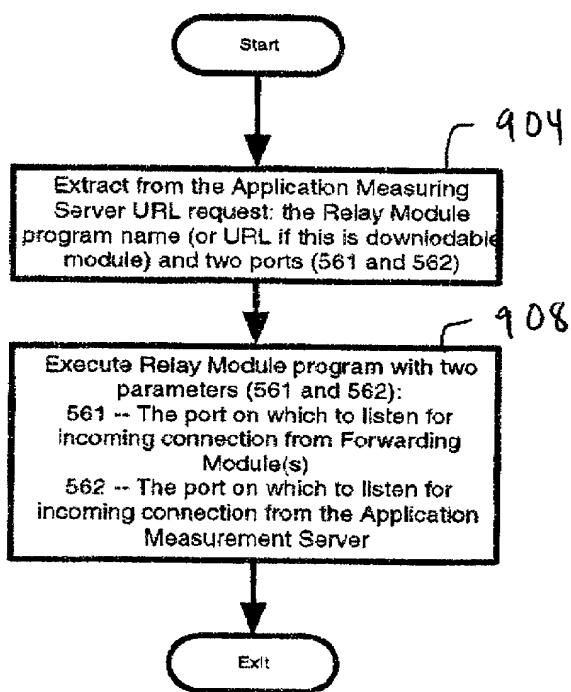


FIG. 9

```
graph TD
    Start([Start]) --> 1004[Obtain two port numbers (561 and 562) from input parameters (set by Instantiation Module)]
    1004 --> 1008[Listen on port 562 for connection from Application Measurement Server.  
Note: This connection should stay open.]
    1008 --> 1014[Connect on port 561 (Forwarding Module)]
    1014 --> 1018[Read data on port 561 (from Forwarding Module)]
    1018 --> 1024[Write data on port 562 (to Application Measurement Server)]
    1024 --> 1028[Read data on port 562 (from Application Measurement Server)]
    1028 --> 1034{Data received}
    1034 -- Yes --> 1038[Write data on port 561 (to Forwarding Module)]
    1038 --> 1044[Disconnect from port 561 (Forwarding Module)]
    1034 -- No --> 1044
    1044 --> 1014
```

The flowchart illustrates the process of the Application Measurement Server. It begins with a 'Start' terminal, leading to step 1004: 'Obtain two port numbers (561 and 562) from input parameters (set by Instantiation Module)'. This is followed by step 1008: 'Listen on port 562 for connection from Application Measurement Server. Note: This connection should stay open.' The process then moves to step 1014: 'Connect on port 561 (Forwarding Module)'. Step 1018: 'Read data on port 561 (from Forwarding Module)' follows, leading to step 1024: 'Write data on port 562 (to Application Measurement Server)'. Step 1028: 'Read data on port 562 (from Application Measurement Server)' leads to a decision diamond 1034: 'Data received'. If the answer is 'Yes', the flow proceeds to step 1038: 'Write data on port 561 (to Forwarding Module)'. If the answer is 'No', the flow proceeds directly to step 1044: 'Disconnect from port 561 (Forwarding Module)'. Both paths from step 1038 and the 'No' path from step 1034 lead to step 1044, which then loops back to step 1014.

FIG. 10

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

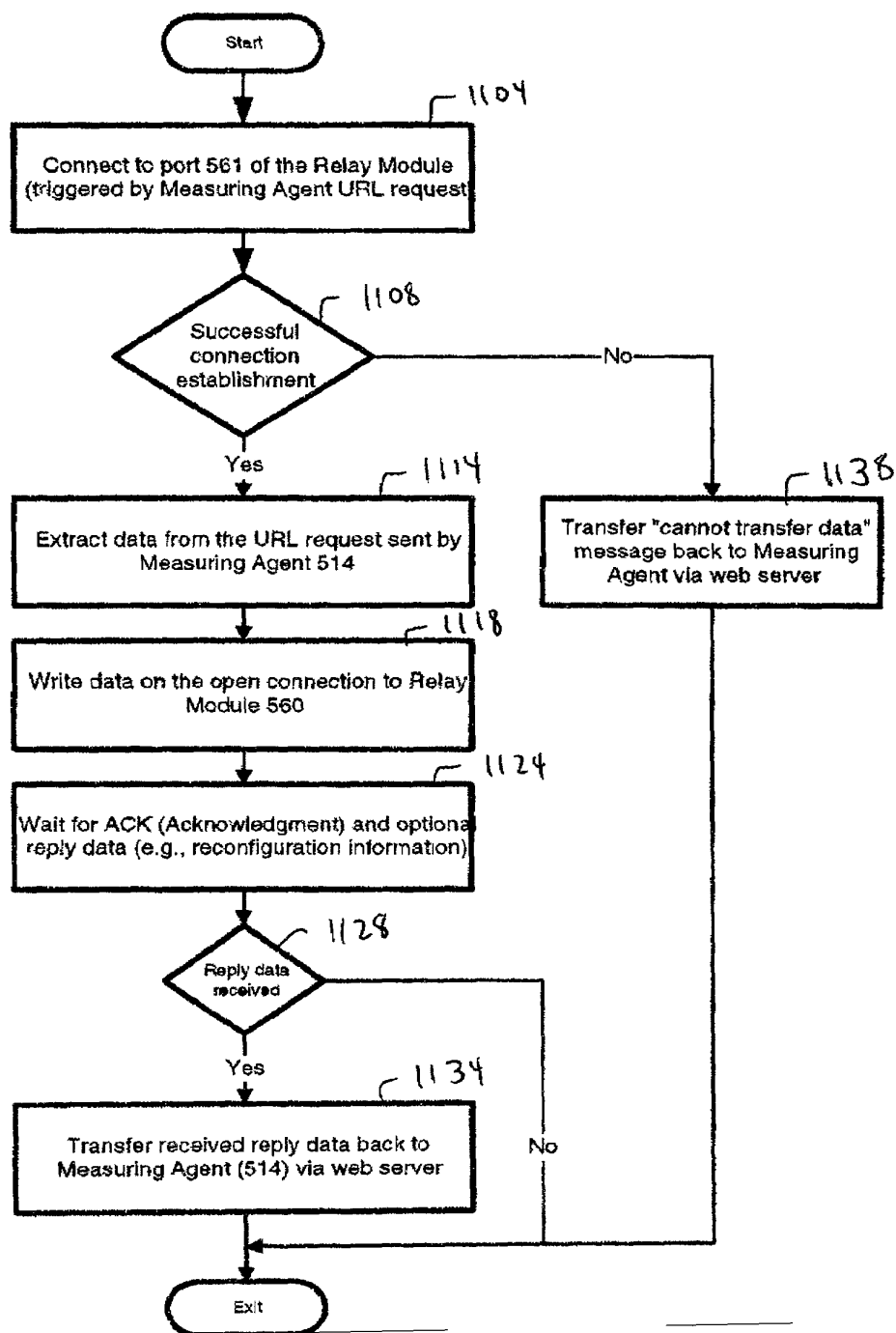


FIG. 11

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION**ATTORNEY DOCKET NO. 10992668-1

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Secure Data Transfer Method And System

the specification of which is attached hereto unless the following box is checked:

() was filed on _____ as US Application Serial No. or PCT International Application
Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

Foreign Application(s) and/or Claim of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			YES: _____ NO: _____
			YES: _____ NO: _____

Provisional Application

I hereby claim the benefit under Title 35, United States Code Section 119(e) of any United States provisional application(s) listed below:

APPLICATION SERIAL NUMBER	FILING DATE

U. S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (patented/pending/abandoned)

POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

Customer Number **022879**Place Customer
Number Bar Code
Label here

Send Correspondence to:
HEWLETT-PACKARD COMPANY
 Intellectual Property Administration
 P.O. Box 272400
 Fort Collins, Colorado 80528-9599

Direct Telephone Calls To:

Thomas Li
 (650) 857-5972

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Inventor: Slawomir K. IlnickiCitizenship: USResidence: 27349 Julietta Lane Los Altos, CA 94022Post Office Address: Same as residence

Inventor's Signature

Date

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION (continued)**

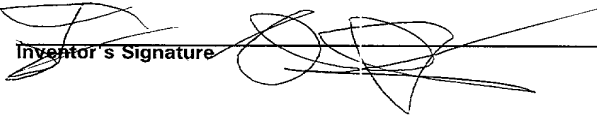
ATTORNEY DOCKET NO. 10992668-1

Full Name of # 2 joint inventor: Troy Shahoumian

Citizenship: US

Residence: 1269 Poplar Ave., #107, Sunnyvale, CA 94086

Post Office Address: Same as residence

Inventor's Signature

Date

6/7/00

Full Name of # 3 joint inventor: _____

Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____

Date _____

Full Name of # 4 joint inventor: _____

Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____

Date _____

Full Name of # 5 joint inventor: _____

Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____

Date _____

Full Name of # 6 joint inventor: _____

Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____

Date _____

Full Name of # 7 joint inventor: _____

Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____

Date _____

Full Name of # 8 joint inventor: _____

Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature _____

Date _____